VISUAL REVIEW | Vol. 17, No. 8, 2025 | ISSN 2695-9631
International Visual Culture Review / Revista Internacional de Cultura Visual
https://doi.org/10.62161/revvisual.v17.5806

CYBERSECURITY FACTORS IN METAVERSE GAMES IN CHILDREN AND TEENAGERS

ZULEMA DARIA LEIVA BAZAN[1]
zleiva@uch.edu.pe
JULIO CÉSAR MENDEZ-NINA[1]
jmendez@uch.edu.pe

[1] University Association of Sciences and Humanities, Peru

KEYWORDS

Metaverse games
Metaverse
Cybersecurity
Threats
Online games
Children
Teenagers

ABSTRACT

This study aimed to analyse the cybersecurity factors in metaverse games among children and teenagers based on 64 articles sourced from Scopus. It concludes that minors constitute the most significant number of users who disregard real-world rules. Children are the most vulnerable, with boys being more prone to addiction and girls being at higher risk. In the video game environment, preventive education is insufficient, as is the ability to detect cyber threats, which are considered minor offences. Online games increase interaction and information, foster innovation, and improve behaviour. Threats are classified as sexual, fraudulent, and those that violate dignity. Suitable regulations and active participation are recommended; understanding, analysis, and knowledge of dangers, along with the provision of resources, are deemed necessary.

Received: 23/ 03 / 2025
Accepted: 17/ 06 / 2025

1. Introduction

We are experiencing one of the greatest crises in human history; the paradigm shift intensified following the COVID-19 pandemic, which spurred the advancement of technologies, including immersive ones, transforming services and communication. This new scenario, far from being viewed negatively, should be understood as an opportunity for growth (Winterhalter, 2023). Advanced information and communication technologies (ICT) have achieved transformative and constant effects across various aspects of life: from ethical and economic consequences to cultural, sustainable, and scientific changes (Padilla et al., 2023). This rapid and continuous development has altered the way things are done, inviting all stakeholders to collaborate in harnessing the advantages of cyberspace (Cano, 2022).

Parallel to technological progress, the metaverse has emerged, an environment that integrates disciplines such as 3D modelling, animation, cloud computing, blockchain, artificial intelligence (AI), and next-generation internet applications. It comprises Extended Reality (XR), encompassing Augmented Reality (AR) and Mixed Reality (MR), configuring spaces where the physical, human, and digital worlds converge, creating interconnected environments (Dwivedi et al., 2022). Another classification is provided by Lee and Gu (2022), who argue that the metaverse integrates four categories: augmented reality, life logging, as well as mirror and virtual worlds. The latter, based on virtual, mixed, and extended realities, represents an alternative reality like, yet distinct from, the real world. These are, therefore, simulations that connect to produce an enhanced version of the fusion of the physical and digital. In summary, based on this taxonomy, the metaverse is established through its environment, interface, interactions, and social value. Its consolidation has been driven by digital natives and Generation Z users, who adopt the role of prosumers in this field (Barrio, 2023; Crespo et al., 2023), and it will solidify with alpha users.

In this new space, users engage in various activities and are generally represented by avatars, in a process termed personalisation, where individuals interact according to their expectations and interests. Immersion occurs through augmented meta-levels, based on codes and languages. It is anticipated that in the future, it will offer new uses and benefits, heralding an unbounded environment with broad application and development prospects. The metaverse is an expanded system that groups social networks, games, and communities; spaces where advanced interactions merge with real-life experiences, offering opportunities to construct new and improved forms of communication (Bruni et al., 2023; Jim et al., 2023; Wang et al., 2022). On the other hand, social networks have become part of the daily activities of millions of users. In 2023, they played a role in the lives of two-thirds of the global population, establishing themselves as one of the most significant spaces for integration and communication on a worldwide scale. This is particularly evident among children and teenagers, who enjoy videos, share images, and react positively, often more actively, to disseminated content. Advanced communication represents interaction spaces that foster learning, knowledge of cultures, and new lifestyles. They are also considered entertainment tools, with video games standing out as the most popular, providing recreation while potentially attracting risks to the mental and physical health of users (Cabeza-Ramírez et al., 2022; Ramírez-Plascencia et al., 2022).

In this regard, gamification is defined as the use of elements, procedures, approaches, or activities based on game principles and applied in various contexts. It is considered a novel strategy, particularly in the field of sports. These advantages have made video games one of the most influential entertainment media (Navarro et al., 2021; Rodríguez et al., 2022). According to Palma et al. (2022), video games emerged in the early 1970s with the introduction of arcade machines and the first consoles.

The first eSports tournament took place in 1972 at Stanford University; subsequently, in the 1980s, companies like Sega, Atari, and Nintendo popularised domestic consoles through large-scale national and international tournaments. In the 1990s, the internet enabled players to interact with others, subsequently boosting multiplayer competitions. As a result, video games such as *Battlefield*, *Quake*, the *Warcraft* series, *EA Sports FIFA*, among others, gained significant popularity. By the end of the twentieth century, with the progress of new technologies and the support of professional developers, video games expanded their scope, improving the organisation of tournaments, structure, and prizes. This was followed by a surge in the sale of web-based technological devices, driven by the growing number of players, due to the recreational capabilities of video games, attracting major sponsorships to tournaments, including from corporations such as Samsung, Microsoft, ATI, AMD, and others.

Traditional media became involved by broadcasting the World Series; later, the consolidation of transmedia processes with streaming platforms and video-on-demand services followed. Today, online games are on par with sports and socialisation activities, as well as the professionalisation of the competitive video game world. There is a growing interest in online games among both users and spectators. An exponential increase in video game usage is evident; by 2021, the number of players reached 3,000 million, a 5.3% rise from 2020. Currently, online video games compete with physical sports and other socialisation events. They have positioned themselves among the most impactful immersive media, due to their captivating content (Cabeza-Ramírez et al., 2022; Ortega-Jiménez et al., 2023).

Video games encompass all types of electronic or digital programmes that involve interaction across various platforms. Access is facilitated through some form of screen, along with equipment and portable devices, including consoles and arcade platforms (Xbox, PlayStation, Game Boy). They are also accessible via mobile phones, joysticks, rooms, and video display devices (e.g., virtual reality (VR) headsets and mixed reality devices). The latter are advanced and related to AI. They are classified into eight genres: action, adventure, fighting, puzzle, role-playing, simulation, sports, and strategy; these often overlap and/or combine, with the first two being the most favoured (Asadzadeh et al., 2024; Palma et al., 2022). The integration of virtual and augmented realities with gamification gives rise to spaces targeted at minors, highlighting applications such as Sandbox, Roblox, Minecraft, Illuvium, Axie Infinity, Fortnite, and others. The appeal of immersive games is notable, but they also provide opportunities for anonymous cybercriminals to act (Chamorro et al., 2023).

In this context, Latin America is the region with the greatest digital disadvantage, where cyber-attacks increased by 40% over the last five years, equating to over 700 million incidents. The lack of protection stems from limited awareness of threats, the use of outdated applications, gaps in critical infrastructure, low training levels, and legislation that does not penalise cybercrimes (Flores et al., 2023; Kosevich, 2020; Parra & Concha, 2021). Positive aspects include advancements in cybersecurity within AI to counter malicious threats, improvements in risk identification and resolution. In this regard, immersive games offer resources that ensure the privacy and security of information, though these still require configuration (Martínez, 2021; Padilla et al., 2023).

Futuristic environments pose challenges for security preservation; although 5G technology is an effective option, it also presents risks related to the violation of user privacy. Consequently, virtual and augmented realities require a reliable network to enable real-time interaction, as well as an efficient identity generation through authentication that responds to the sensory fusion of signals collected by portable devices and the verification of this data. Additionally, the work of developers and specialists is needed to more accurately disseminate the benefits of these new biometric technologies (Al-Sharafi et al., 2023; Hortal, 2023; Jim et al., 2023).

General Objective

The primary objective of this study is to analyse the cybersecurity factors in metaverse games among children and teenagers.

Specific Objectives

- To identify the status of immersive online games among minors.
- To recognise the benefits of metaverse games among children and teenagers.
- To identify the primary threats to minors in this type of game.
- To highlight solutions to mitigate risks in immersive games.

2. Methodology

In the current context of the importance of cybersecurity, the need arises to analyse its factors in immersive video games. This study is framed within a qualitative approach, based on a systematic literature review (SLR). A four-phase process (identification, selection, choice, and analysis of literature) was implemented, given its structured and clear nature, which enhances reproducibility and minimises bias.

Manterola et al. (2013) indicate that a systematic review aims to conduct an exhaustive and detailed investigation of existing evidence on a specific topic. It is carried out using a standardised protocol, which facilitates the identification of reliable and accurate data, enabling the evaluation of the quality and sensitivity of scientific knowledge. Its systematic nature reduces bias, contributing to the structuring of information (Samnanni et al., 2017).

This analysis followed the PRISMA guidelines, which, according to Moher et al. (2009), are represented in a diagram illustrating the process of inclusion and exclusion of previous studies (Page et al., 2021). The scientific source utilised was Scopus, from which 64 publications were selected, prioritising works from the last decade to ensure the inclusion of the most recent approaches (Figure 1).

A. Bibliographic Search and Identification of Studies

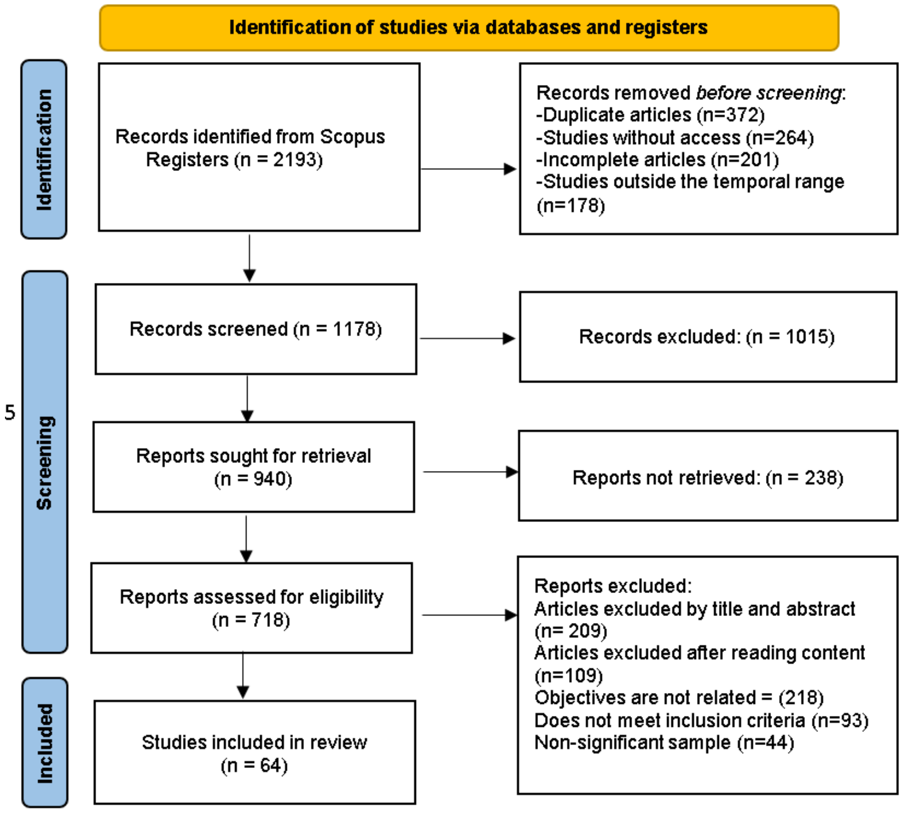
Studies on cybersecurity in metaverse video games between 2014 and 2025 were selected and thematically analysed. Incomplete investigations were excluded, generating various factors and sub-themes from the systematic literature review (SLR), considering the importance of information related to factors impacting security in online video games. This article serves as a precedent for academics and security professionals on the topic, arriving at an understanding of articles from 2014 to 2025 to establish what has been researched and what requires further exploration.

B. Selection of Articles

Initially, 2,193 articles were reviewed, of which those not related to cybersecurity were excluded. The process concluded with the selection of 64 sources for the systematic literature review. A total of 2,193 studies were identified, from which 1,015 records were removed: 372 due to duplication; 264 due to lack of access (unavailable); 201 due to incompleteness; and 178 due to being too outdated. Subsequently, 1,015 investigations were excluded: additionally, 238 studies were not retrieved; 209 were separated based on title and abstract; 109 and 218 were excluded due to unrelated content and objectives; 93 did not meet inclusion criteria; and 44 were removed due to non-significant sample size.

C. Choice

Figure 1. Selected articles

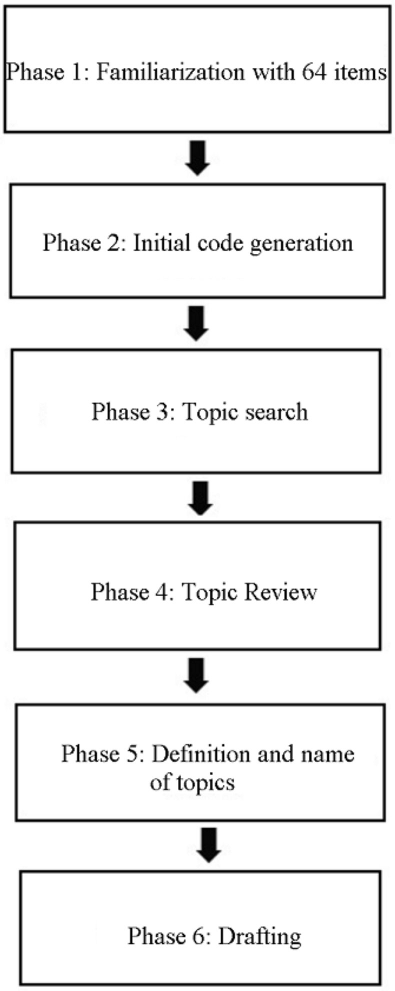

Identification of studies via databases and registers
Identification
Records identified from Scopus Registers (n = 2193)
Records removed *before screening*:
-Duplicate articles (n=372)
-Studies without access (n=264)
-Incomplete articles (n=201)
-Studies outside the temporal range (n=178)
Screening
5
Records screened (n = 1178)
Records excluded: (n = 1015)
Reports sought for retrieval (n = 940)
Reports not retrieved: (n = 238)
Reports assessed for eligibility (n = 718)
Reports excluded:
Articles excluded by title and abstract (n= 209)
Articles excluded after reading content (n=109)
Objectives are not related = (218)
Does not meet inclusion criteria (n=93)
Non-significant sample (n=44)
Included
Studies included in review (n = 64)

Source: Scopus database, 2014-2025.

D. Analysis

The factors and sub-themes were subsequently identified using the model proposed by Braun and Clarke (2006), which involves a series of stages outlined in Figure 2. The selected literature was analysed with the aim of recognising the agents of cybersecurity within gaming applications. Finally, sub-categories were obtained. Duplicate sub-categories and codes were removed with the support of experts in the field.

Figure 2. Stages of information analysis


Phase 1: Familiarization with 64 items
Phase 2: Initial code generation
Phase 3: Topic search
Phase 4: Topic Review
Phase 5: Definition and name of topics
Phase 6: Drafting

Source: Scopus database, 2014-2025.

Below is a list of the 64 studies from the Scopus database, detailed according to country, year of publication and area of focus.

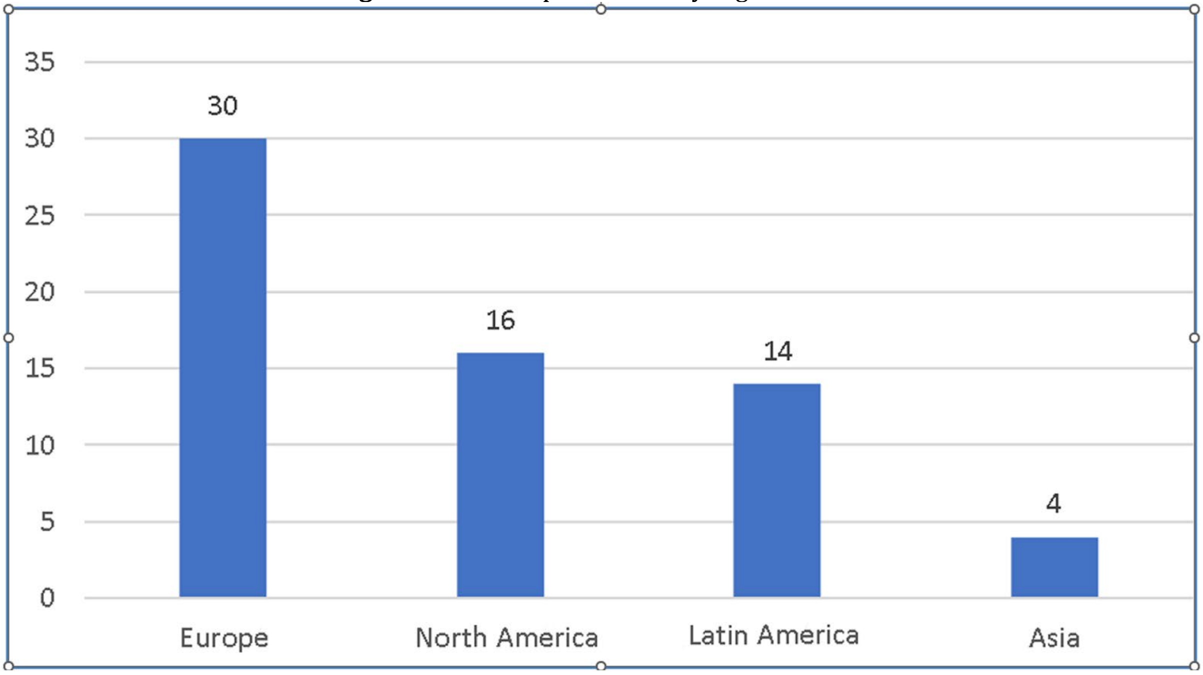
Table 1. Subjects addressed in selected articles

Authors	Topic	Number
Cano (2022), Cervel (2023), Criollo-C et al. (2024), Falchuk et al. (2021), Faraz et al. (2022), Flores et al. (2023), Kang et al. (2023), Kim et al. (2023), Kosevich (20222), Lena-Acebo et al. (2022), Lopez et al. (2020), Martinez et al. (2024), Padilla (2023), Quayyum et al. (2021), Riega et al. (2023), Rodriguez and Palomo (2023), Sommer et al. (2023), Wang et al. (2022).	Cybersecurity	18
Asadzadeh et al. (2024), Calli & Ediz (2023), Camacho (2023), Da Silva et al. (2019), Del Moral (2016), Guerra - Antequera (2024), Hou et al. (2023), King (2023), Lluch et al. (2022), López et al. (2022), Martin (2023), Navarro et al. (2021), Palma (2022), Rodrigues et al. (2019), Rodríguez et al. (2022), Ruiz-Bañuls (2021), Valencia (2022).	Gamification	17
Al-Sharafi et al. (2023), Bruni et al. (2023), Chamorro-Atalaya et al. (2023), Crespo-Pereira et al. (2023), Dwivedi et al. (2022), Jim et al. (2024), Kshetri (2022), Lee and Gu (2023), Lee & Kim (2022), Patan and Parizi (2023), Oz (2023), Rangel (2022), Winterhalter (2023).	Metaverse	13
Astorga-Aguilar & Schmidt-Fonseca (2019), Cabeza-Ramírez et al. (2022), Dzomira (2023), França et al. (2022), Gómez-Quintero et al. (2022), López-Belmonte (2020), Martínez et al. (2021), Ortega et al. (2023), Qamar and Afzal (2023), Talapuru et al. (2023), Trejos and Peláez (2023).	Threats in video games	11
Barrio (2023), Ester (2018), Klein et al. (2019), Parra & Concha (2020), Ramirez-Plascencia et al. (2022),	Cybersecurity legislation	5

Source: Selected articles from Scopus database, 2014-2025.

Table 1 shows that the most analysed topic in the selection of articles is "cybersecurity," with 18 studies; followed by "gamification," with 17; research on "metaverse" stands out next; while "threats in video games" are addressed in 11; and finally, the topic of "legislation in cybersecurity" is covered in 5 articles.

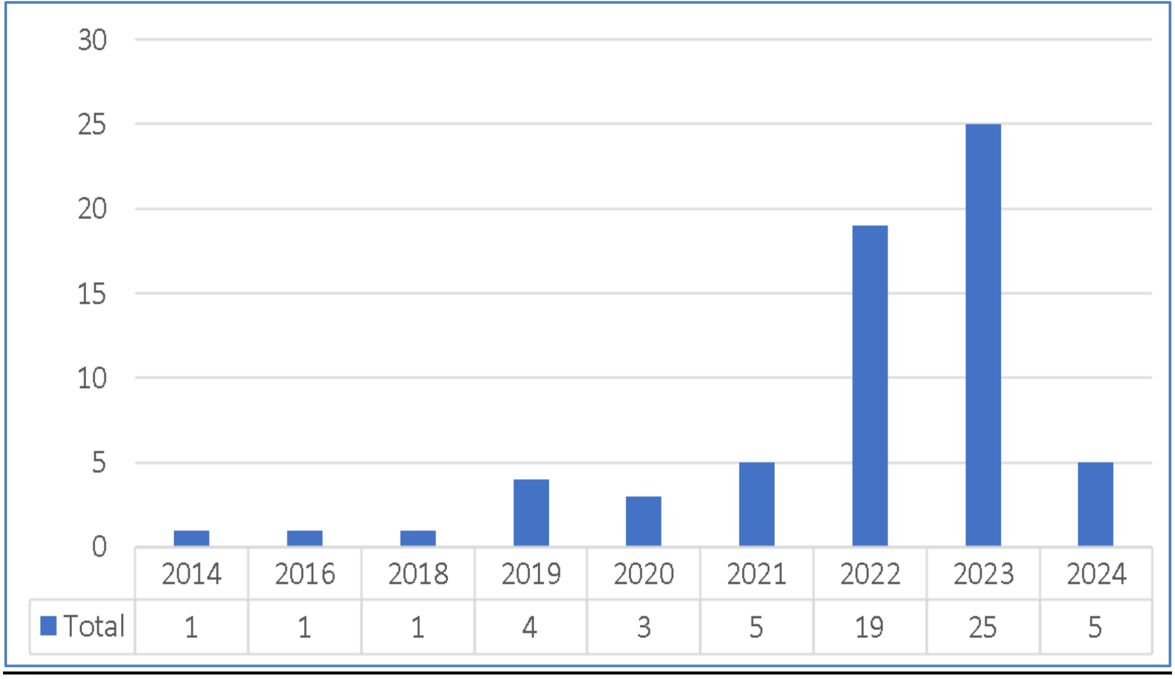
Figure 3. Articles publication by region



Source: Selected articles from Scopus database, 2014-2025.

Figure 3 illustrates that the continent contributing the highest number of publications on cybersecurity in video games for minors is Europe, with 30 articles; followed by North America (United States), with 16 publications; in third place, Latin America with 14; and finally, Asia, which accounts for 4 studies.

Figure 4. Publication of articles by year



	2014	2016	2018	2019	2020	2021	2022	2023	2024
■ Total	1	1	1	4	3	5	19	25	5

Source: Selected articles from Scopus databas, 2014-2025.

Regarding the years in which studies on security in online video games were published, 2023 has the highest number of articles, totalling 25; followed by 2022, with 19; then 2024 and 2021, with 5 studies each; finally, the years 2024, with 4; 2020, with 3; and 2018, 2016, and 2014, with 1 article each, respectively.

3. Results

The primary purpose of this study is to analyse the cybersecurity factors in metaverse games among minors; the results obtained from this analysis are detailed below.

3.1 Situation of Cybersecurity in Metaverse Games among Minors

Currently, two irreconcilable perspectives coexist regarding metaverse games. One views them as a valuable and socially useful tool, while the other considers them mere entertainment with potential risks. Concerning the latter stance, it is crucial to evaluate the reliability of immersive applications due to imbalances between reality and the virtual environment, as well as to design necessary improvements. In this regard, the most common complaints about advanced gaming applications include low reliability, persistent threats, lack of credibility, and the increased scope of dangers, generating insecurity and rejection (Calli & Ediz, 2023 Jim et al., 2023; Winterhalter, 2023).

Children and teenagers represent the largest number of participants in online games, as they prefer the fun and freedoms offered by virtuality over their well-being, often disregarding real-world rules. On the other hand, teenagers are more susceptible to developing addiction problems, particularly in shooting and role-playing games, where interaction with other players can intensify these issues through mechanisms such as levels, points, and badges that sustain user attention and increase playing time (França et al., 2023; Hou et al., 2022; Ruiz-Bañuls et al., 2021; Wang et al., 2022).

This reality demonstrates that, depending on the age and gender of users, differences in digital behaviour exist. Regarding the first criterion, children exhibit a higher level of privacy vulnerability compared to teenagers, who are more aware of the information they share. Starting to play at an early age increases problems such as addiction and future exposure to inappropriate content. As age advances, the frequency of engagement with these gaming environments increases, and consequently, so do the associated risks. In a significant percentage, young children use digital platforms to inform and share personal content, whereas teenagers focus on gaining greater recognition to enhance self-representation and facilitate social connections (Hou et al., 2022; Lena et al., 2022).

Regarding gender, males engage more frequently with video games due to the rewards and satisfaction they derive, which impacts their lack of control—a symptom linked to addiction tendencies. Likewise, males tend to participate more intensely in multiplayer programmes. Conversely, females are more involved in actions against norms, as they exhibit a higher degree of unawareness regarding their actions (Cabeza-Ramírez et al., 2022; Nilupu et al., 2023; Ortega-Jiménez et al., 2023).

The most popular gaming platforms, notably Twitch and YouTube Gaming, highlight social interaction as a key element, encouraging users to extend their time spent on these platforms. Regarding preferred devices, smartphones, PCs, and PlayStation facilitate access to a wide variety, including action and adventure encounters, which attract many participants. Users face dangers such as addiction, cyberbullying, and exposure to violent or pornographic content, leading to negative consequences like neglect of responsibilities, inability to manage time, and the emergence of family and social conflicts (Cabeza-Ramírez et al., 2022; Hou et al., 2022).

Currently, global governance is being constructed on the internet, a setting where the primary threats originate from powers in the northern hemisphere, specifically the United States (U.S.) and the European Union (EU). The approach to cybersecurity varies across these two regions. In the U.S., priority is given to surveillance and global control, granting it the greatest capacity for espionage and online attacks. In contrast, the EU structures supranational legislation, focusing on the prevention, punishment, and prosecution of internet crimes, necessitating constant evaluation and adaptation of responses. Notable jurisdictions include Spain and Germany (Hurel, 2022; Mejía-Lobo et al., 2023; Perafán Del Campo et al., 2021; Seoane, 2022).

In Latin America, the level of cybersecurity is lower compared to other regions, revealing insufficient preparedness to address cyber risks, although gradual progress is observed (Kosevich, 2020). Efforts include Peruvian legislation, which anticipates and counters cybercrime. In Chile, both laws and critical digital infrastructure fail to provide protection against attacks. Similarly, Colombian regulations exhibit significant shortcomings in classifying these offences (López et al., 2021; Mejía-Lobo et al., 2023; Queirolo et al., 2021;).

Concerning the understanding of threats in immersive games, most users possess technical skills but lack the maturity to reflect on risks. A culture of prevention is acquired at an early age, explaining why many minors misconfigure their profiles or share information (França et al., 2023; Lena et al., 2022; Quayyum et al., 2021). Other concerns include the lack of resources dedicated to security by companies, the absence of preventive measures among staff, and the lack of tools to detect dangers (Dzomira, 2014).

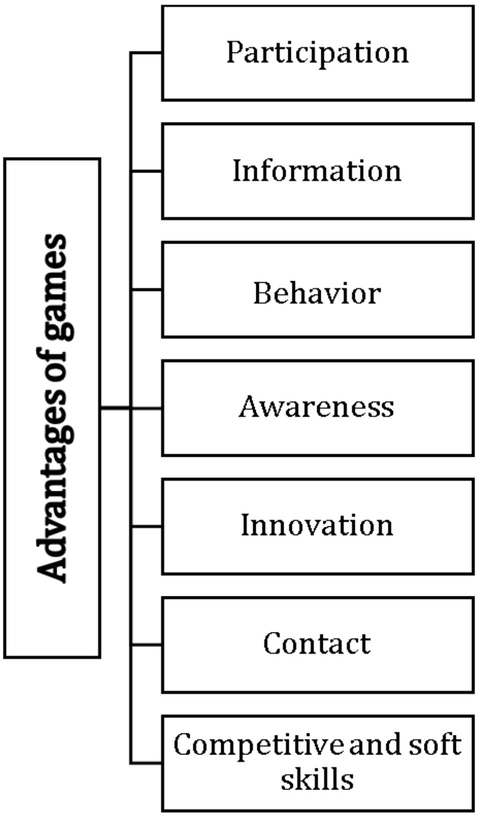
Addiction to video games can be linked to a lack of attention and a distant relationship between parents and children. Other causes include a lack of awareness among minors about dangers, as well as a low perception of risk, which increases vulnerability during instances of bullying and other online threats. This poses a legal challenge, as regulations governing AI use vary by region, leading to inconsistencies in the application of protective measures (Hou et al., 2022; Ramírez-Plascencia et al., 2022).

The convergence of artificial intelligence with crime has altered the nature of attacks, exploiting weaknesses without detection. Some users behave appropriately in real life but act otherwise in virtual environments due to the absence of strict regulation. On the other hand, victims of cyberbullying do not fit a single profile; they include individuals intimidated in person, as well as popular users vulnerable in fragile social contexts. Furthermore, the dynamics of roles are complex, where victims may become aggressors and vice versa. The impact of bystanders is significant: some remain indifferent, others defend the victim, and some even support the aggressor, legitimising their behaviour and status. For these reasons, prevention and regulation are considered major challenges (Flores et al., 2023; Martín, 2022).

3.2 Advantages of Metaverse Games

The consolidation of the metaverse across various digital platforms entails a series of changes and challenges. Nevertheless, it also generates numerous benefits, particularly in the realm of gaming, as detailed below.

Figure 5. Advantages of metaverse games



Source: Selected articles from Scopus database, 2014-202.

A. Participation

Gamification, through avatars and other elements, promotes positive exchange and interaction among users; moreover, thanks to immersion, players can socialise and engage in recreational activities. In this context, social media applications establish themselves as spaces for interaction and integration, facilitating connections between users and acting as agents of cohesion within digital communities (Bruni et al., 2023; Kim et al., 2023; Ramírez-Plascencia et al., 2022). Likewise, video games stand out as socialisation environments, thanks to the organisation of popular events that foster relationships through networks of friendship and contacts. However, this dynamic requires users to invest a significant amount of time (Palma et al., 2022; Ruiz-Bañuls et al., 2021).

B. Information

Metaverse games are regarded as tools for disseminating information, as they facilitate the transfer of knowledge, capturing interest through their novel content, including 3D experiences (Valencia, 2022). This transmission of data strengthens knowledge and communication skills, while encouraging cooperation (Silva et al., 2019). Consequently, over the past decade, the metaverse has emerged as an increasingly significant global communication agent, and one effect of the widespread use of social media is that children and teenagers have become more active consumers of information. Furthermore, this information can be integrated into curricular content, promoting cooperative learning and the discovery of other cultures and lifestyles (Asadzadeh et al., 2024).

C. Behaviour

Gamification in the metaverse transfers elements of virtuality into the real world, influencing behaviour, particularly among children, by replacing undesirable conduct such as negligence or indifference towards potential threats with greater awareness and concern for these risks. Metaverse games guide the improvement of students' behaviour, as attitudes are significant in understanding and predicting social conduct (Crespo et al., 2023; Quayyum et al., 2021).

An attitude is a behavioural pattern that responds to conditioned stimuli based on social experiences, particularly in the case of minors through the content of metaverse games. Furthermore, these games foster collaborative attitudes and behaviours by developing dynamics aimed at modifying certain negative conducts (Da Silva et al., 2019; López-Belmonte et al., 2020; Ruiz-Bañuls et al., 2021).

D. Awareness

Motivation derived from immersive experiences increases awareness of cybersecurity, contributing to the sensitisation of existing dangers and facilitating changes in minors' behaviour. This is a notable benefit of entertainment applications. Its success stems from the fun associated with gaming, as gamification enhances the effort exerted by minors (Kim et al., 2023; Oz, 2023; Ramírez-Plascencia et al., 2022). It encourages the performance of tasks in pursuit of recognition, prompting reflection and interest in learning. Introducing video games at an early stage promotes the achievement of objectives, capturing attention and creating a conducive environment for the development of skills and competencies (Asadzadeh et al., 2024; Guerra-Antequera et al., 2022).

E. Innovation

Gamification applications based on artificial intelligence develop skills in design and mimicry, stimulating innovation and creativity as players seek alternatives to navigate these environments, linking knowledge and skills to provide solutions. Creativity is nurtured through play, particularly during childhood and adolescence—stages where entertainment holds a central role. Watching videos, sharing images, and reacting to content have become primary forms of recreation (Del Moral & Guzmán, 2016; Lluch-Molins et al., 2022; Valencia, 2022; Oz, 2023).

F. Contact

The metaverse, through its personalised avatars, offers a range of advantages for connecting with other users, providing closeness with loved ones and the preservation of memories, even after death. Additionally, it enables remote work activities and reduces physical contact for health protection.

G. Competitive Skills

Video games are characterised by fostering a competitive spirit. Their selection inherently involves self-imposed challenges, and online confrontation allows players to measure and compare their abilities, a hallmark of eSports (Guerra-Antequera et al., 2022; Palma et al., 2022; Ruiz-Bañuls et al., 2021). These challenges promote collaborative learning, as advanced technology connects knowledge and skills to deliver solutions. It is also essential to adopt more appealing challenges that permit mistakes while monitoring progress and updating reward strategies (Lluch-Molins et al., 2022; López-Belmonte et al., 2020).

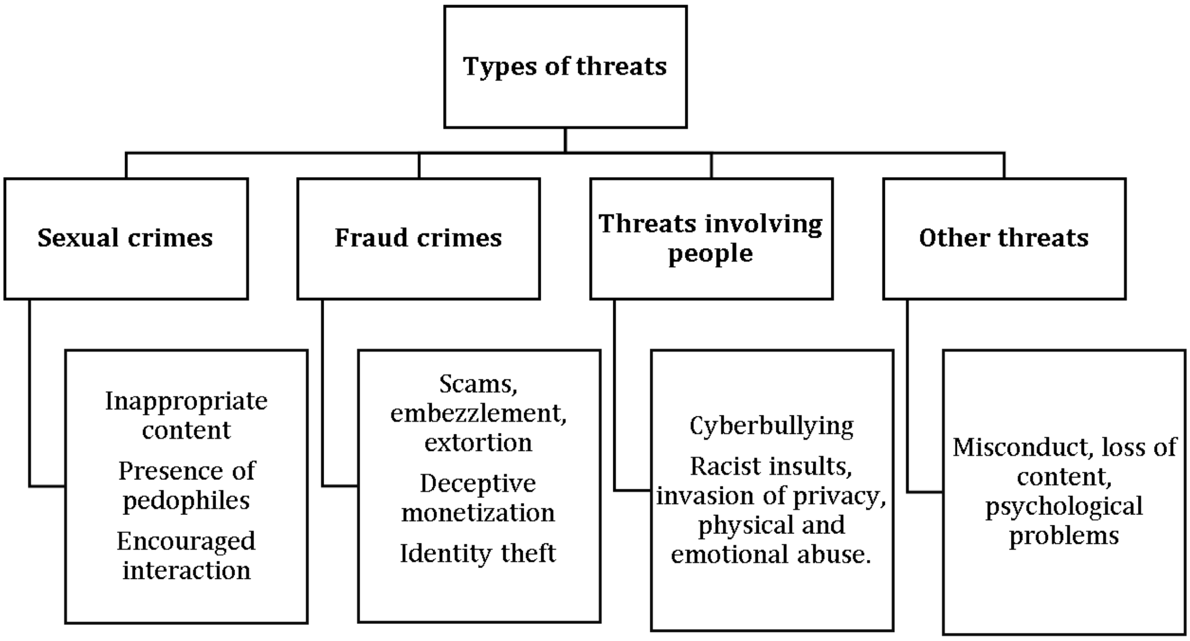
H. Soft Skills

Video games cultivate essential soft skills for successful performance in life and work. These include commitment, teamwork, individual and collective decision-making, cooperative learning, and problem-solving (Palma et al., 2022; Ruiz-Bañuls et al., 2021). Furthermore, video games enhance the development of fine motor skills, as success in eSports requires optimal coordination. They compete with physical sports, promote healthy habits, and strengthen mental abilities. On the other hand, the advancement of streaming platforms enables players to improve their practice, as observing others enriches the experience, aiding in the refinement of skills (Asadzadeh et al., 2024; Cabeza-Ramírez et al., 2022; Guerra-Antequera et al., 2022).

3.3 Types of Threats

The convergence of advanced technologies in areas such as social, political, economic, military, and entertainment domains has rendered them vulnerable to cyber-attacks (Flores et al., 2023; Kosevich, 2020). Consequently, the dangers associated with online metaverse games are classified as follows: sexual crimes, fraud offences, threats against the person, and others (Qamar & Afzal, 2023).

Figure 6. Types of threats in metaverse games.



Source: Selected articles from Scopus database, 2014-2025.

A. Sexual Crimes

Among these offences, the most prevalent include inappropriate content for minors, the presence of paedophiles, malicious interactions between children and adults, pornography, sexual harassment, and online dating. In the game Roblox, notable issues include grooming of minors, dissemination of sexual material, rape threats, among others (Calli & Ediz, 2023; França et al., 2023).

B. Fraud Offences

Regarding frauds, the most frequent include identity theft, bitcoin scams, financial embezzlement, deceptive monetisation in freemium models, gambling hoaxes, identity impersonation, unregulated economic spaces, extortion, among others (King, 2023; Qamar & Afzal, 2023).

C. Threats Against the Person

Concerning threats against the person, users are exposed to cyberbullying, racist insults, privacy invasion, recruitment and radicalisation of ideas, and, of course, verbal and/or physical violence. Additionally, social and technological issues arise, such as digital inequality, exclusion, exposure to computer viruses, physical location detection, addiction, technological dependence, isolation, etc. (França et al., 2023; Quayyum et al., 2021).

D. Other Threats

Other frequent threats include emotional manipulation and narrative coercion. Likewise, social misconduct, loss of personal content, and other psychological issues within the metaverse are considered. There has been an increase in offences related to immersive games, particularly those of a sexual nature and frauds, which violate individuals' dignity and rights (Calli & Ediz, 2023; Ester, 2023; King, 2023). The most common danger for minors is cyberbullying, which often begins as a game. The sense of power and anonymity provided by the online world amplifies criminality.

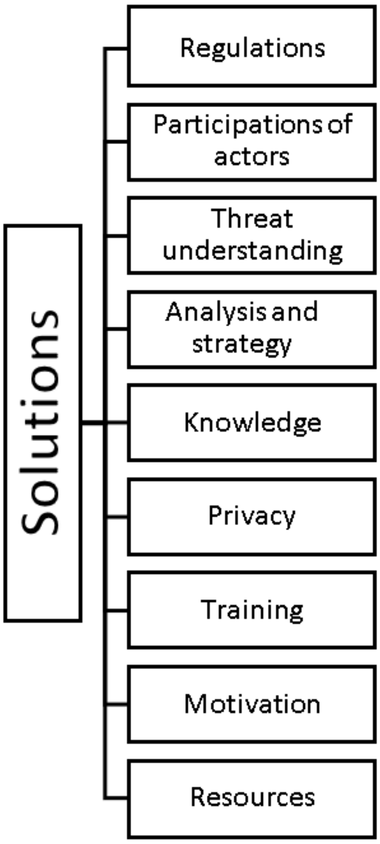
These criminal acts present greater risks and are addressed with increased complexity. In this scenario, developers face an excessive volume of real-time requests (Talapuru et al., 2023; Trejos & Peláez, 2023). Excessive time spent on online games leads to difficulties in social adaptation, resulting in behavioural issues such as aggression or hurtful comments. Attitudes that disrupt the digital environment may even escalate to physical aggression. Furthermore, excessive interaction with video games increases the likelihood of mental health problems, such as depression and social anxiety.

Other threats of a physiological nature include reduced quality of life and sleep, as well as somatic disorders (Cabeza-Ramírez et al., 2022; Hou et al., 2022). Additionally, academic difficulties emerge, including lower school performance, neglect of important tasks, etc. Regarding technological risks, notable issues include addiction to games, mobile pornography, cyber aggression, web violence, harassment, victimisation, dissemination of inappropriate content, and the rapidly widening socio-technological generational gap (Palma et al., 2022; Ramírez-Plascencia et al., 2022).

3.4. Solutions Against Threats in the Metaverse

Cybersecurity in the metaverse must prioritise an integrated approach, encompassing regulations, collaboration among stakeholders, and ongoing education. Therefore, the following solutions are proposed from various key perspectives:

Figure 7. Solutions against threats in metaverse.



Source: Selected articles from Scopus database, 2014-2025.

A. Regulations

Technological advancements necessitate the adaptability of regulatory systems with respect to risks. These must be legally governed through standardised, certified, and transparently applied norms, particularly in the operations of private companies. Additionally, supervision and monitoring by regulatory bodies are required to ensure reliability and security in the metaverse, aligning with the challenges of Industry 4.0, the needs of businesses, and societal expectations (Bruni et al., 2023; França et al., 2023; Ilárraz & Palomo, 2023; Klein et al., 2022; Parra & Concha, 2021; Sommer et al., 2023; Wang et al., 2022).

In European legislation, cybersecurity is addressed through a non-interventionist approach, prioritising sovereignty in cyberspace. In Latin America, it is imperative that cybercrimes are adjudicated with a specialised focus. This requires the implementation of a legal framework that enables the prevention, prosecution, and punishment of these offences (Hortal, 2023; Trejos & Peláez, 2023).

The application of sanctions should consider the age of offenders, encouraging a willingness to avoid reoffending and fostering learning from the offence committed, while avoiding extreme penalties and opting for mediation mechanisms. Governments must establish age-restriction policies to protect children (Hou et al., 2022; Martín, 2022). Furthermore, a unified international legal approach is demanded, empowering competent authorities to perform their duties (Payá-Santos & Luque Juárez, 2021).

B. Participation of Stakeholders

Cybersecurity is not solely the responsibility of governments and technology companies; it requires the active involvement of public and private organisations, families, communities, media outlets, and academic institutions. Collaboration among stakeholders is essential to establish standards and protocols, fostering trust in the metaverse (Crespo et al., 2023; Falchuk et al., 2018; Jim et al., 2023).

Consequently, engaging stakeholders is imperative, necessitating collaboration among engineering, security, and professional protection organisations. This involvement integrates technology, individuals, and process changes. Convening better-trained analysts equipped with cutting-edge technological tools is urgent to address the high volume of cyber-threats, which not only affect security but also citizens' rights (Payá-Santos & Luque Juárez, 2021).

Regarding close agents, such as parents, relatives, and friends, their support proves valuable in preventing potential video game usage disorders. It is recommended that parents actively engage with their children's web usage, fostering good relationships and understanding their gaming behaviours to mediate effectively (Cabeza-Ramírez et al., 2022; Dzomira, 2014; Martínez et al., 2024).

C. Understanding of Threats

It is essential to comprehend the criminal nature of dangers in online games and to take actions to counteract them, establishing boundaries and responsibilities to prevent them. Adolescents perceive risk as the ability to recognise and respond to conflict situations arising from internet interactions. It is necessary for minors to understand the dangers to which they are exposed (Gómez et al., 2024; Martín, 2022).

It is vital to strengthen informative policies to efficiently comprehend augmented communications, recognising their risks. Likewise, creating reporting and follow-up mechanisms is necessary to manage dangers appropriately. Coexistence in cyberspace should focus on citizen participation to reduce misinformation, manipulation, and other threats (Cano, 2022; Falchuk et al., 2018).

D. Analysis and Strategy

As with any strategic process, security in metaverse games requires a rigorous audit (Wang et al., 2022). Based on this exploration, a protection architecture is designed, tailored to the primary challenges and the characteristics of each application. This architecture relies on secure data exchange, authentication, proximity, encryption, and the use of blockchain (Kang et al., 2024; Patan & Parizi, 2023).

In recent years, the use of artificial intelligence (AI) has gained increasing relevance in security due to its ability to counter potential threats by identifying and mitigating risks. Due to its speed, this technology accelerates the analysis of large volumes of data to detect any possible threat, while also identifying system imperfections. This automates defence mechanisms, reducing human intervention; however, it must be addressed by various coordinated agents (Padilla et al., 2023; Rafael, 2023).

E. Knowledge

The level of awareness regarding online cyberbullying correlates with the degree of prevention. Therefore, it is necessary to seek, contrast, or recognise false information about a critical state to anticipate it (Nilupu et al., 2023). Online protection and security depend on users' awareness of risks, especially when sharing information, configuring privacy, or deleting content. Acquiring preventive knowledge early and continuously is essential. Moreover, the role of parents is crucial for safe development in the digital environment (Astorga & Schmidt, 2019; Lena et al., 2022).

G. Privacy

In the face of latent dangers, the best preventive approach is to anticipate any vulnerability. Actions should be capable of initiating, controlling, monitoring, persisting, and assessing their effectiveness while being encoded into the game and compatible with avatars. In this regard, privacy in these digital spaces must be managed by specialists who ensure the proper functioning of platforms (Gómez et al., 2024; Falchuk et al., 2018).

H. Training

Training is the most widely used approach for protection, recommended through content tailored to young audiences, such as comics, animations, graphic novels, and social media experiences. Thus, it is essential to promote critical digital education among minors from an early age. Through training, minors develop protective skills and judgement against dangers like identity theft and cyberbullying, the latter being the most frequent risk in recent years (Martín, 2022; Quayyum et al., 2021; 2022).

Another valuable suggestion is the use of gamification in security content. However, this poses a challenge for parents, who must adapt to innovations in digital communication to guide minors (Criollo et al., 2024; Martínez, 2021). If organisations opt to invest in the metaverse, they must manage, among other aspects, the training of human resources. This process is complemented by specialised external support, including the adoption of a value proposition, the establishment of viable objectives, and the evaluation of technological risks (Bruni et al., 2023).

I. Motivation

Motivation is a key aspect in increasing knowledge about cyber-threats among minors. The metaverse offers realistic experiences that develop awareness, modifying preventive attitudes towards dangers. Therefore, it is necessary to design and manage efficient solutions for immersive spaces. This encourages minor participation, making it an effective strategy to reduce threats such as cyberbullying and victimisation (Hou et al., 2022; Quayyum et al., 2021).

J. Resources

Currently, the investment allocated to security in the metaverse is substantial; therefore, it is important for companies, businesses, and end users to manage these resources to achieve a reliable and sustainable immersive environment, recognising the social value of ethical technology and concern for the digital environment. This ensures optimal cybersecurity, allowing everyone to enjoy this space safely (Bruni et al., 2023; Crespo et al., 2023; França et al., 2023).

4. Conclusions

The primary objective of this study was to analyse the cybersecurity factors in metaverse games among children and teenagers. Regarding the risk situation in these applications, minors constitute the largest number of participants, often disregarding real-world rules. The metaverse is a valuable tool but presents threats. Offences have increased, with children experiencing higher vulnerability. During adolescence, risks intensify as recognition is sought. Males are prone to addiction, while females are more involved in risky actions. Participants possess technical skills but lack preventive and reflective training. The most popular platforms are Twitch and YouTube Gaming, with preferences for smartphones, PCs, and PlayStation.

In Latin America, cybersecurity is inferior to other regions. There is a lack of resources and detection tools. Cybercrimes are often treated as administrative offences. Regulations for artificial intelligence (AI) vary by region. Anonymity provides advantages to criminals. Addiction is linked to attention issues and poor parent-child relationships. Victims may become aggressors. Threats in the metaverse for minors are categorised as: sexual crimes, such as inappropriate content, the presence of paedophiles, pornography, etc.; in Roblox, grooming and fraud offences proliferate; threats against the person, including cyberbullying, the most prevalent danger; and other threats, such as privacy invasion and emotional manipulation.

Among the advantages of metaverse games: they promote active participation due to their interactive nature, serve as an excellent dissemination channel by sparking interest in immersive content, and foster more responsible behaviours towards threats. They motivate innovation and creativity, facilitate interactive contact, saving time and protecting health. They encourage a competitive spirit by comparing skills, providing problem-solving opportunities, and offering rewards. They develop soft skills, fine motor abilities, mental skills, and improvements in practice. The proposed solutions include oversight by regulators, with cybercrimes adjudicated under standardised norms.

Stakeholders must be active participants. Necessary training is required to raise awareness and prevention, alongside monitoring dangers, designing protection tailored to each application. Significant investment is needed for a reliable, sustainable, and ethical environment, along with informative policies and efficient reporting channels.

The sample of 64 revealed that the selection cannot be generalised. This may introduce bias, so it is recommended to conduct studies on the addressed factors. Likewise, research on cybersecurity across various online entertainment media is suggested. Finally, comparisons of variables by region or continent are proposed, including studies analysing the perception of digital protection among users of other generations.

References

Al-Sharafi, M.A., Al-Emran, M., Al-Qaysi, N., Iranmanesh, M., & Ibrahim, N. (2023). Drivers and Barriers Affecting Metaverse Adoption: A Systematic Review, Theoretical Framework, and Avenues for Future Research. *International Journal of Human–Computer Interaction*, 1–22. https://doi.org/10.1080/10447318.2023.2260984

Asadzadeh, A., Shahrokhi, H., Shalchi, B., Khamnian, Z., & Rezaei-Hachesu, P. (2024). Serious educational games for children: A comprehensive framework. *Heliyon,* 10(6), e28108. https://doi.org/10.1016/j.heliyon.2024.e28108

Astorga-Aguilar C., & Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Revista Electrónica Educare, 23(*3), 339-362. https://dx.doi.org/10.15359/ree.23-3.17

Barrio, M. (2023). El Metaverso y su impacto en el Estado y la soberanía. *Revista de Derecho Político*, (117), 197–220. https://doi.org/10.5944/rdp.117.2023.37925

Braun, V., y Clarke, V. (2006). Uso del análisis temático en psicología. *Investigación cualitativa en psicología*, 3 (1), 12-23.

Bruni, R., Piccarozzi, M., & Caboni, F. (2023). Defining the Metaverse with challenges and opportunities in the business environment. *Journal of Marketing Theory and Practice*, 33 (1), 1–18. https://doi.org/10.1080/10696679.2023.2273555

Cabeza-Ramírez, L.J., Rey-Carmona, F.J., del Carmen Cano-Vicente, M. (2022). Analysis of the coexistence of gaming and viewing activities in Twitch users and their relationship with pathological gaming: a multilayer perceptron approach. *Sci Rep 12*, 7904 https://doi.org/10.1038/s41598-022-11985-0

Calli, B., & Ediz. C. (2023). Top concerns of user experiences in Metaverse games: A text-mining based approach*. Entertainment Computing, 46*, 1-17. https://doi.org/10.1016/j.entcom.2023.100576

Camacho-Sánchez, R., Serna, J., Rillo-Albert, A., & Lavega-Burgués, P. (2023). Enhancing motivation and academic performance through gamified digital game-based learning methodology using the ARCS model. *Interactive Learning Environments*, 1–18. https://doi.org/10.1080/10494820.2023.2294762

Cano, J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova*, 20(40), 815-832. https://dx.doi.org/10.21830/19006586.866

Chamorro-Atalaya, O., Durán-Herrera, V., Suarez-Bazalar, R., Nieves-Barreto, C., Tarazona-Padilla, J., Rojas-Carbajal, M., Cruz-Telada, Y., Caller-Luna, J., Alarcón-Anco, R., & Arévalo-Tuesta, J. (2023). Inclusion of Metaverses in the Development of the Flipped Classroom in the University environment: Bibliometric Analysis of Indexed Scientific Production in SCOPUS. *International Journal of Learning, Teaching and Educational Research, 22*(10). https://doi.org/10.26803/ijlter.22.10.14

Crespo-Pereira, V., Sánchez-Amboage, E., & Membiela-Pollán, M. (2023). Facing the challenges of metaverse: a systematic literature review from social sciences and marketing and communication. *Profesional de la Información*, *32*(1), 1-21. https://doi.org/10.3145/epi.2023.ene.02

Criollo-C., S., Guerrero-Arias, A., Buenaño, D., & Luján-Mora, S. (2024). Usability and Workload Evaluation of a Cybersecurity Educational Game Application: A Case Study. *IEEE Access, 12,* 12771-12784. https://doi.org/10.1109/ACCESS.2024.3352589

Da Silva, J. (2023). Protection, expertise and domination: Cyber masculinity in practice. *Computers & Security*, 133, 103408. https://doi.org/10.1016/j.cose.2023.103408

Del Moral, E., & Guzmán, A. (2016). Jugar en red social: ¿Adicción digital versus comunicación e interacción en CityVille? *Cuadernos.info*, (38), 217-231. http://dx.doi.org/10.7764/cdi.38.810

Dwivedi, Y., Hughes, L., Baabdullah, A., Ribeiro, S., Giannakis, M., Al-Debei, M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D., Gustafsson, A., Hinsch, C., Jebabli, I., . . . Wamba, S. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66, 1–55. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry Zimbabwe. *Risk governance & control financial markets & institutions,* *4*(2), 17-27. https://doi.org/10.22495/rgcv4i2art2

Ester, A. (2023). El desafío de la Inteligencia Artificial a la vigencia de los derechos fundamentales. *Cuadernos Electrónicos de Filosofía del Derecho, 48*, 111-139. http://dx.doi.org/10.7203/CEFD.48.25863

Falchuk, B., Loeb, S., & Neff, R. (2018). The Social Metaverse: Battle for Privacy. *IEEE Technology and Society Magazine*, 37, (2), 52-61. https://doi.org/10.1109/MTS.2018.2826060

Faraz, A., Montsef, J., Raza, A., & Willis, S. (2022). Child Safety and Protection in the Online Gaming Ecosystem. *IEEE Access, 10*, 115895-115913. https://doi.org/10.1109/ACCESS.2022.3218415

França, F., Leitão, B., Santos, J., & Oliveira, M. (2023). O abuso sexual contra crianças e adolescentes no ambientes virtual: o caso do abuso de avatar e os riscos na expansão do metaverso. *Relacoes Internacionais no Mundo Atual,* *4*(42), 102–129. https://revista.unicuritiba.edu.br/index.php/RIMA/article/view/e-5953/371374555

França, F., Leitão, B., Santos, J., & Oliveira, M. (2023). O abuso sexual contra crianças e adolescentes no ambientes virtual: o caso do abuso de avatar e os riscos na expansão do metaverso. *Relacoes Internacionais no Mundo Atual, 4*(42), 102–129.

Gómez-Quintero, J., Johnson, S., Borrion, H., & Lundrigan, S. (2024). A scoping study of crime facilitated by the metaverse. *Futuros, 157*, 1-22. https://doi.org/10.1016/j.futures.2024.103338

Guerra-Antequera, J., Antequera-Barroso, J. A., & Revuelta-Domínguez, F. I. (2022). Degree of motivation and acquisition of visuospatial perception after the incorporation a video game in the learning of mathematical knowledge. *Heliyon,* 8(8), e10316. https://doi.org/10.1016/j.heliyon.2022.e10316

Cervel, M. (2023). Ciberinjerencias en los procesos electorales y el principio de no intervención (una perspectiva internacional y europea). *Revista Electrónica de Estudios Internacionales*, (45). https://dialnet.unirioja.es/servlet/articulo?codigo=9033002

Hou, C. Y., Rutherford, R., Chang, H., Chang, F. C., Shumei, L., Chiu, C. H., Chen, P. H., Chiang, J. T., Miao, N. F., Chuang, H. Y., & Tseng, C. C. (2022). Children's mobile-gaming preferences, online risks, and mental health. *PloS one,* 17(12), e0278290. https://doi.org/10.1371/journal.pone.0278290

Hurel, LM (2022). Interrogando la agenda de desarrollo de la ciberseguridad: Una reflexión crítica. *The International Spectator*, 57 (3), 66–84. https://doi.org/10.1080/03932729.2022.2095824

Ilárraz, C. R., & Zurdo, R. J. P. (2023). Transparencia, ciberseguridad e identidad digital en el entorno 5G. *Revista española de la transparencia,* (18), 359-380. DOI: https://doi.org/10.51915/ret.298

Jim, J., Hosain, M., Mridha, M., Kabir, M., & Shin, J. (2023). Toward Trustworthy Metaverse: Advancements and Challenges. *IEEE Access, 11*, 118318–118347. https://doi.org//10.1109/ACCESS.2023.3326258.

Kang, G., Koo, J., & Kim, Y. G. (2024). Requisitos de seguridad y privacidad para el metaverso: una perspectiva de las aplicaciones del metaverso. *Revista IEEE Communications, 62* (1), 148-154. https://doi.org/10.1109/MCOM.014.2200620

Kim, J.B., Zhong, C., & Liu, H. (2023). Teaching Tip: What You Need to Know about Gamification Process of Cybersecurity Hands-on Lab Exercises: Lessons and Challenges. *Journal of Information Systems Education, 34*(4), 387-405. https://jise.org/Volume34/n4/JISE2023v34n4pp387-405.html

King, J., Fitton, D., & Cassidy, B. (2023). Investigating Players Perceptions of Deceptive Design Practices within a 3D Gameplay Context. *Proceedings of the ACM on Human-Computer Interaction, 7*(407), 876–892. https://doi.org/10.1145/3611053

Klein, V., Domingues, J., & Tajra, G. (2023). Antitruste no metaverso: economia comportamental e o bem-estar do consumidor. *Revista de Defesa da Concorrência, 11*(2). https://doi.org/10.52896/rdc.v11i2.1052.

Kosevich, E. (2020). Cyber Security Strategies of Latin America Countries. *Iberoamericana*, (1) 137-159. https://doi.org/10.37656/s20768400-2020-1-07

Kshetri, N., (2022). Metaverse technologies in product management, branding and communications: virtual and augmented reality, artificial intelligence, non-fungible tokens and brain-computer interface. *Central European Management Journal. (31)*4, 511-521. https://www.emerald.com/insight/2658-0845.htm

Lee, H., & Gu, H. (2022). Empirical Research on the Metaverse User Experience of Digital Natives. *Sustainability, 14*(22). https://doi.org/10.3390/su142214747.

Lee, U.K., & Kim, H. (2022). UTAUT in Metaverse: An "Ifland" Case. *Journal of Theoretical and Applied Electronic Commerce Research, 17*(2), 613–635. https://doi.org/10.3390/jtaer17020032

Lena-Acebo, F.J., Renés-Arellano, P., Hernández-Serrano, M.J., & Caldeiro-Pedreira, M.C. (2022). Knowing how to share and to protect oneself: key factors on digital cybercritical education for children. *Profesional de la información*, *31*(6). https://doi.org/10.3145/epi.2022.nov.09

Lluch, L., Balbontin, F., & Sullivan, N. (2022). Enhancing cooperative learning and student motivation with gamification strategies: A case study in industrial engineering. *Journal of Technology and Science Education, 12*(3), 611-627. https://doi.org/10.3926/jotse.1693

López-Belmonte, J., Segura, A., Fuentes, A., & Parra, M. (2020). Evaluating Activation and Absence of Negative Effect: Gamification and Escape Rooms for Learning. *International Journal of Environmental Research and Public Health, 17*(7). https://doi.org/10.3390/ijerph17072224

López-Noguero, F., Gallardo-López, J., & Muñoz-Villaraviz, D. (2022). Videojuegos y preadolescencia. Uso, hábitos e implicaciones socioeducativas en función del género. *Revista Colombiana de Educación, 1*(84), 1-25. https://doi.org/10.17227/rce.num84-12701

López, FA, Ruete, D., Gatica, G. (2021). Infraestructura crítica y ciberseguridad en Chile: Lineamientos para el consenso. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, (E43), 41–55. https://www.risti.xyz/issues/ristie43.pdf

Manterola, C.; Astudillo, P.; Arias, E. & Claros, N. (2013). Systematic reviews of the literature: what should be known about them. *Cir. Española Journal,* 91(3):149-55. DOI: 10.1016/j.cireng.2013.07.003

Martín, N. (2022). Estudio del conocimiento de los menores sobre las consecuencias de sus actuaciones en las Redes Sociales. *Doxa Comunicación.* Revista Interdisciplinar De Estudios De Comunicación Y Ciencias Sociales, 35, 419. http://hdl.handle.net/10637/13798

Martínez, F., Sánchez, L., Santos-Olmo, A., Rosado, D., & Fernández, E. (2024). Maritime cybersecurity: protecting digital seas. *Revista Internacional de Seguridad de la Información, 23*(2), 1429–1457. https://doi.org/10.1007/s10207-023-00800-0

Martínez, J., Lareki, A., & Altuna, J. (2021). Risks Associated with Posting Content on the Social Media. *Revista Iberoamericana de Tecnologías del Aprendizaje, 16*(1) 77-83. https://doi.org/10.1109/RITA.2021.3052655

Mejía-Lobo, M., Hurtado-Gil, S. V., y Grisales-Aguirre, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista de Ciencias Sociales*, XXIX (2), 356-372. https://doi.org/10.31876/rcs.v29i2.39981

Moher, D., Liberati, A., Tetzlaff, J., Altman, DG y PRISMA Group. (2009). Elementos de informe preferidos para revisiones sistemáticas y metanálisis: la declaración PRISMA*. Annals of Internal Medicine*, 151(4), 264-269. DOI: 10.1016/j.jclinepi.2009.06.005

Navarro, C., Pérez, I., & Marzo, P. (2021). La gamificación en el ámbito educativo español: revisión sistemática (Gamification in the Spanish educational field: a systematic review). *Retos, 42*, 507–516. https://doi.org/10.47197/retos.v42i0.87384

Padilla, R., Ojeda, A. y Sanchez, C. (2023). Issues in Information Systems Navigating the business landscape: challenges and opportunities of implementing artificial intelligence in cybersecurity governance. *Issues in Information Systems,* 24(4), 328-338. https://doi.org/10.48009/4_iis_2023_125

Page, M., McKenzie, J., Bossuyt, P., Boutron, I., Hoffmann, T., Mulrow, C., Shamseer, L., Tetzlaff, J., Akl, E., Brennan, S., Chou, R., Glanville, J., Grimshaw, J., Hróbjartsson, A., Lalu, M., Li, T., Loder, E., Mayo-Wilson, E., McDonald, S., …Moher, D. (2021). Declaración PRISMA 2020: una guía actualizada para la presentación de informes de revisiones sistemáticas. *PLOS Medicine*, 18(3), e1003583. https://doi.org/gjpmcj

Palma-Ruiz, J. M., Torres-Toukoumidis, A., González-Moreno, S. E., & Valles-Baca, H. G. (2022). An overview of the gaming industry across nations: using analytics with power BI to forecast and identify key influencers. *Heliyon,* 8(2), Artículo e08959. https://doi.org/10.1016/j.heliyon.2022.e08959

Parra, D., y Concha, R. (2021). Inteligencia artificial y derecho. Problemas, desafíos y oportunidades. *Vniversitas*, 70, 1–25. https://doi.org/10.11144/Javeriana.vj70.iadp

Payá-Santos, C., & Luque Juárez, J. M. (2021). El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. *Revista Científica General José María Córdova*, 19(36), 1121-1136. https://dx.doi.org/10.21830/19006586.855

Ortega-Jiménez, D., Cedeño-González, G., & Ramírez, M. (2023). Uso problemático de videojuegos y flexibilidad de afrontamiento en adolescentes ecuatorianos. *Health and Addictions/ Salud y Drogas, 23*(1), 289-301. https://doi.org/10.21134/haaj.v23i1.748

Perafán Del Campo, E.A., Polo Alvis, S., Sánchez Acevedo, M.E., & Miranda Aguirre, C. (2021). Estado y soberanía en el ciberespacio. *Via Inveniendi Et Iudicandi,* 16(1). https://doi.org/10.15332/19090528.6480

Oz, B. (2023). A new perspective in construction management; the metaverse. *Revista De La Construcción. Journal of Construction, 22*(2), 321-336. https://doi.org/10.7764/RDLC.22.2.321.

Patán, R., & Parizi, R. (2023). Securing Data Exchange in the Convergence of Metaverse and IoT Applications. *ACM International Conference Proceeding Series,* (129), 1-8. https://doi.org/10.1145/3600160.3605019

Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Comput. Secur. 128*, 1-22. https://doi.org/10.1016/j.cose.2023.103127

Quayyum, F., Cruzes, D., & Jaccheri, M. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction, 30*, 1-25. https://doi.org/10.1016/j.ijcci.2021.100343

Queirolo, F., Matheu, A., Ruff, C., Juica, P., Ruiz, M. (2021). El 5G como vector de soberanía nacional: oportunidades y desafíos. *Revista Ibérica de Sistemas e Tecnologias de Informação*; Lousada. (E46), 28-43.

Ramírez-Plascencia, D., Alonzo-González, R. y Marín-Tapiero, J. (2022). Youtubers menores de edad y sus riesgos frente a los vacíos legales en México. *Revista Mediterránea de Comunicación,* 13(1), 65-77. https://www.doi.org/10.14198/MEDCOM.20781

Rangel, C. (2022). Inteligencia Artificial como aliada en la supervisión de contenidos comerciales perjudiciales para menores en Internet. *Revista Mediterránea de Comunicación, 13*(1), 17-30. https://www.doi.org/10.14198/MEDCOM.20749

Riega-Virú, Y., Nilupu-Moreno, K., Salas-Riega, J., & Ninaquispe, M. (2023). Knowledge of cybersecurity against social cybercrime of female high school students. *Education and Research*. 1-4 https://doi.org/10.1109/ICALTER61411.2023.10372927

Rodrigues, R., Gouveia, R., & Pereira, C. (2019). Gamification in Management Education: A Systematic Literature Review. *BAR - Revista de la Administración Brasileña, 16*(2). https://doi.org/10.1590/1807-7692bar2019180103

Rodríguez, A., Vicente, E., De Mena, J., & Pérez, S. (2022). Efecto de la práctica de actividad física gamificada en el estado de ánimo de jugadoras de baloncesto en etapa de confinamiento (Effect of gamified physical activity practice on the mood of female basketball players in confinement stage). *Retos, 43*, 10–16. https://doi.org/10.47197/retos.v43i0.87177

Rodríguez, C., & Palomo, R. (2023). Transparencia, Ciberseguridad e Identidad Digital en el Contexto 5G | Transparencia, ciberseguridad e identidad digital en el entorno 5G. *Revista Española de la Transparencia*, (18), págs. 359–380. https://doi.org/10.51915/ret.298

Ruiz-Bañuls, M., Gómez-Trigueros, I.M., Rovira-Collado, J., Rico-Gómez, M.L. (2021). Gamification and Transmedia in Interdisciplinary Contexts: A Didactic Intervention for the PrimarySchool Classroom, *Heliyon,* 7 (6), https://doi.org/10.1016/j.heliyon.2021.e07374.

Samnani, S., Vaska, M., Ahmed, S. & Turin, T. C. (2017). Review typology: the basic types of reviews for synthesizing evidence for the purpose of knowledge translation. *J. Coll. Physicians Surg. Pak*., 27(10):635-41. https://www.jcpsp.pk/archive/2017/Oct2017/10.pdf

Silva, R. J. R. da, Rodrigues, R. G., & Leal, C. T. P. (2019). Gamification in management education: A systematic literature review. *Brazilian Administration Review*, 16(2), e180103. https://doi.org/10.1590/1807-7692bar2019180103

Seoane, M. V. (2023). La ciberhegemonía de EE. UU. en la OEA. Estudos Internacionais. *Revista De relações Internacionais da PUC Minas*, 10(4), 91–112. https://doi.org/10.5752/P.2317-773X.2022v10n4p91-112

Sommer, U., Matania, E., & Hassid, N. (2023). The rise of companies in the cyber era and the pursuant shift in national security. *Political Science, 75*(2), 140-164. https://doi.org/10.1080/00323187.2023.2278499

Talapuru, S., Dantu, R., Upadhyay, K., Badruddoja, S., & Zaman, S. (2023). The Dark Side of the Metaverse: Why is it Falling Short of Expectations? *2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA),* 287-296. https://doi.org/10.1109/TPS-ISA58951.2023.00043

Trejos-Gil, C., & Peláez-Vélez, Y. (2023). Ciberdelitos en menores de edad en la red social Facebook: revisión sistemática de literatura. *Nuevo Derecho, 19*(32), 1–18. https://doi.org/10.25057/2500672X.1493

Valencia, L. (2022). Implementación de estrategias gamificadas en el marco de la comunicación organizacional. *Revista Internacional de Cultura Visual, 7*(10), 1-11. https://doi.org/10.37467/revvisual.v9.3623

Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T., & Shen, X. (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials, 25*(1), 319-352. https://doi.org/10.1109/COMST.2022.3202047

Winterhalter, C. (2023). Metaverse and Its Communication. The Future is Here. True or False? en: Sabatini, N., Sádaba, T., Tosi, A., Neri, V., Cantoni, L. (eds.), Fashion Communication in the Digital Age. FACTUM 2023. *Proceedings in Business and Economics* (37-48). https://doi.org/10.1007/978-3-031-38541-4_4